L Number	Hits	Search Text	DB	Time stamp
1	1	("5442705").PN.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 07:36
2	77	@ad<19990831 and ((carry adj up) with add$5)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 07:43
3	1	(@ad<19990831 and ((carry adj up) with add$5)) and (??cipher$3 ??crypt$3)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 07:41
5	0	(@ad<19990831 and ((carry adj up) with add$5)) and (key adj expan$5)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 07:42
7	0	(@ad<19990831 and ((carry adj up) with add$5)) and (DES FEAL)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 07:42
8	896	@ad<19990831 and ((shift$3) with (prime))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 07:46
12	176	@ad<19990831 and ((relative$3 adj prime))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 07:45
13	11	@ad<19990831 and (shift$3 with (relative$3 adj prime))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 07:46
14	47	@ad<19990831 and ((shift$3) with (prime)) and (??crypt$3 ??cipher$3)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 07:58
19	0	@ad<19990831 and ((shift$3) with (relatively adj prime)) and (??crypt$3 ??cipher$3)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 07:57
20	47	@ad<19990831 and (((shift$3) with (prime)) "relatively prime") and (??crypt$3 ??cipher$3)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 07:58
53	93	@ad<19990831 and ("XOR" "exlusive-or" "exclusive or") and (key adj2 (transform$7 expan$5 exten$5)) and constant	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 08:22
54	0	(shift$3 rotat$3) and (relatively adj prime)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 08:22
55	25	((380/44).CCLS.) and ((380/29).CCLS.)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 08:22
57	123	@ad<19990831 and ("XOR" "exlusive-or" "exclusive or") and (key adj2 (transform$7 expan$5 exten$5)) and (shift$3 rotat$3)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 08:23
59	66	"des" same (key adj expansion)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/17 08:23
61	98	"carry-up"	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 08:23

56	1	(("5442705").PN.) and (shift$3 rotat$3)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 08:23
58	6	"relatively prime"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/17 08:23
60	8	"des" near (random adj3 generator)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/08/17 08:23
62	11	("carry-up" same (add addition subtract$3)) and @ad<20000831	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 08:23
63	26	((("5442705").PN.) (@ad<19990831 and ((carry adj up) with add$5)) ((@ad<19990831 and ((carry adj up) with add$5)) and (??cipher$3 ??crypt$3)) ((@ad<19990831 and ((carry adj up) with add$5)) and (key adj expan$5)) ((@ad<19990831 and ((carry adj up) with add$5)) and (DES FEAL)) (@ad<19990831 and ((shift$3) with (prime))) (@ad<19990831 and ((relative$3 adj prime))) (@ad<19990831 and (shift$3 with (relative$3 adj prime))) (@ad<19990831 and ((shift$3) with (prime)) and (??crypt$3 ??cipher$3)) (@ad<19990831 and ((shift$3) with (relatively adj prime)) and (??crypt$3 ??cipher$3)) (@ad<19990831 and (((shift$3) with (prime)) "relatively prime") and (??crypt$3 ??cipher$3)) (@ad<19990831 and ("XOR" "exlusive-or" "exclusive or") and (key adj2 (transform$7 expan$5 exten$5)) and constant) ((shift$3 rotat$3) and (relatively adj prime)) (((380/44).CCLS.) and ((380/29).CCLS.)) ((("5442705").PN.) and (shift$3 rotat$3)) (@ad<19990831 and ("XOR" "exlusive-or" "exclusive or") and (key adj2 (transform$7 expan$5 exten$5)) and (shift$3 rotat$3)) "relatively prime" ("des" same (key adj expansion)) "carry-up" ("des" near (random adj3 generator)) (("carry-up" same (add addition subtract$3)) and @ad<20000831)) and @pd>20040301	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 08:27

64	Lwk + ABS (previous search (results updated)	4	((("5442705").PN.) (@ad<19990831 and ((carry adj up) with add$5)) ((@ad<19990831 and ((carry adj up) with add$5)) and (??cipher$3 ??crypt$3)) ((@ad<19990831 and ((carry adj up) with add$5)) and (key adj expan$5)) ((@ad<19990831 and ((carry adj up) with add$5)) and (DES FEAL)) (@ad<19990831 and ((shift$3) with (prime))) (@ad<19990831 and ((relative$3 adj prime))) (@ad<19990831 and (shift$3 with (relative$3 adj prime))) (@ad<19990831 and ((shift$3) with (prime)) and (??crypt$3 ??cipher$3)) (@ad<19990831 and ((shift$3) with (relatively adj prime)) and (??crypt$3 ??cipher$3)) (@ad<19990831 and (((shift$3) with (prime)) "relatively prime") and (??crypt$3 ??cipher$3)) (@ad<19990831 and ("XOR" "exlusive-or" "exclusive or") and (key adj2 (transform$7 expan$5 exten$5)) and constant) ((shift$3 rotat$3) and (relatively adj prime)) (((380/44).CCLS.) and ((380/29).CCLS.)) (((("5442705").PN.) and (shift$3 rotat$3)) (@ad<19990831 and ("XOR" "exlusive-or" "exclusive or") and (key adj2 (transform$7 expan$5 exten$5)) and (shift$3 rotat$3)) "relatively prime" ("des" same (key adj expansion)) "carry-up" ("des" near (random adj3 generator)) (("carry-up" same (add addition subtract$3)) and @ad<20000831)) and @pd>20040301 and @ad<19990831	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 08:29
65	ABS	1	("20040049678").PN.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 08:29

09652157
Michael J. Simitoski
Michael.Simitoski@uspto.gov
(703) 305-8191

Google

blowfish "key expansion" XOR (shift OR shifting) DES
blowfish "key expansion" XOR (shift OR shifting) DES "relatively prime"
"key expansion" (shift OR shifting) "relatively prime"
"key expansion" "relatively prime"

ACM

"key expansion"
"key expansion" +XOR +shift shifting
"key expansion" +transform +substitution

IEEE

"key expansion"
xor <and> shift <and> (key <and> (expand <or> expansion))
relatively prime <and> ('des' feal encryption ciphertext)

Other

Search tool	Search Terms

Applications/Patents from Inventor Search

Web Images Groups News Froogle more »

relatively-prime shift OR shifting "key expar Search Advanced Search Preferences

Web Results **1** - **26** of about **39** for **relatively-prime shift OR shifting "key expansion "**. (**0.15** seconds)

[PDF] 1 Cryptography
File Format: PDF/Adobe Acrobat - View as HTML
... The **shift** offsets C1, C2 and C3 depend on the ... obtained by key schedule which involves **key expansion** and key ... a small odd integer E that is **relatively prime** to O ...
www.ece.purdue.edu/~sbagchi/Research/ ReadingGroup/issa_sensorcryptography_041703.pdf - Similar pages

[PDF] Cryptography for Smalltalkers Cryptography for Smalltalkers
File Format: PDF/Adobe Acrobat - View as HTML
...1 built from simple, fast operations (xor, **shift**, x + y ... patented, royalty-free l 2 parts: **key expansion** & data ... primes p, q public: e = **relatively prime** to (p-1 ...
www.smalltalksolutions.com/ smalltalksolutions/pdf/Kobetic.pdf - Similar pages

[PPT] CSCE 790: Computer Network Security
File Format: Microsoft Powerpoint 97 - View as HTML
... hence 8 and 15 are **relatively prime**. 9/4/2003. 21. ... byte substitution works on bytes using a table of 256 entries. **shift** rows is simple byte **shifting**. ...
www.cse.sc.edu/~huangct/CSCE790F03/lecture5.ppt - Supplemental Result - Similar pages

[PDF] RIJNDAEL dvanced ncryption tandard
File Format: PDF/Adobe Acrobat - View as HTML
... C2 bytes and Row 3 over C3 bytes The **shift** offsets C1 ... which exists since c(x) was chosen **relatively prime** to x ... the key K, we expand it via **Key Expansion** and get ...
www.math.uiuc.edu/~domazet/rijndael.pdf - Similar pages

RSA Security -
... **key expansion** A process that creates a larger key from the ... LFSR linear feedback **shift** register. ... **relatively prime** Two integers are **relatively prime** if they have ...
www.rsasecurity.com/rsalabs/node.asp?id=2373 - 58k - Cached - Similar pages

nCipher Security Resources: Glossary
... **key expansion** A process that creates a larger key ... See also linear feedback **shift** register ... **relatively prime** reverse engineer To ascertain the functional basis of ...
www.ncipher.com/resources/downloads/sr_glossary.php - 86k - Cached - Similar pages

[PS] Scalable Block Ciphers Based on Feistel-like Structure
File Format: Adobe PostScript - View as Text
... **prime** to m. 0. ... The **key expansion** algorithm is based on the lagged Fibonacci generator with L ... 3) - MYWORD.BITS)) #define **SHIFT** 17 #define COMPL.**SHIFT** (MYWORD.BITS ...
www.exp-math.uni-essen.de/~trung/SBC.ps - Similar pages

[PS] Quantum Cryptography: a new hope
File Format: Adobe PostScript - View as Text
... cypher where a message is encoded by **shifting** (modulo 26 ... is more difficult to break than the **shift** cypher, but ... If m and n are **relatively prime**, it's easy to see ...
www.iro.umontreal.ca/~paquin/Qu/quantumCrypto.ps - Similar pages

[PDF] CRYPTOGRAPHY AND DATA SECURITY A Short Course
File Format: PDF/Adobe Acrobat - View as HTML
Page 1. ECE428 Computer Networks and Security W'2004 GB Agnew These notes are for use by registered students in ECE428 and may ...

www.ece.uwaterloo.ca/~ece428/notes_2004.pdf - Supplemental Result - Similar pages

[PPT] Chapter 2 Introduction to Cryptography
File Format: Microsoft Powerpoint 97 - View as HTML
... f(a) = ak mod n (k and n are **relatively prime**) When n = 26 and k = 9 ... 每一個round 的**shift** bit數為(1, 0), (2, 1), (3, 2), (4, 2), (5, 2), (6, 2 ... **Key Expansion**. ...
140.114.78.121/~mikemouse/course/Chapter3.ppt - Similar pages

United States Patent Application: 0040049468 (cited on EAST)
... 0=x.sup.2 mod n random integer **relatively prime** to n ... recent counterpart FCSRs (Feedback with Carry **Shift** Registers ... from XORing the key, or from **shifting** the data ...
appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO2& Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-... - 101k - Cached - Similar pages

United States Patent Application: 0040049678
... and x is a random integer **relatively prime** to n ... recent counterpart FCSRs (Feedback with Carry **Shift** Registers) [44 ... from XORing the key, or from **shifting** the data ...
appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO2& Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-... - 101k - Cached - Similar pages
[More results from appft1.uspto.gov]

[PDF] Glossary of Terms
File Format: PDF/Adobe Acrobat - View as HTML
... key exchange A process used by two more parties to exchange keys in cryptosystems. **key expansion** A process that creates a larger key from the original key. ...
www.certicom.com/download/aid-93/glossary.pdf - Similar pages

[PDF] Signatures Digital Signatures The Arbiter Does this work?
File Format: PDF/Adobe Acrobat - View as HTML
... k , such that • k has not been used before • k is **relatively prime** to p ... 23 CSC331 Legend ⊕ - bit-wise EXCLUSIVE OR <<< - cyclic left **shift** ¬ - bit-wise ...
www.cs.ncl.ac.uk/modules/1999-2000/ csc331/notes/Digital%20Signatures.pdf - Supplemental Result - Similar pages

[PDF] Signatures Digital Signatures The Arbiter Does this work?
File Format: PDF/Adobe Acrobat - View as HTML
... such that • k has not been used before • k is **relatively prime** to p ... Slide 23 CSC331 Legend ⊕ - bit-wise EXCLUSIVE OR <<< - cyclic left **shift** ¬ - bit-wise ...
www.cs.ncl.ac.uk/modules/2000-01/ csc331/notes/Digital%20Signatures.pdf - Supplemental Result - Similar pages

My Portal Inc. ::
... **key expansion** – расширение ключа; создание ... linear feedback **shift** register ... **relatively prime** – относительно простое ...
www.myportal.ru/crypt_doc4.html - 55k - Cached - Similar pages

[PDF] RSA Labs FAQ
File Format: PDF/Adobe Acrobat - View as HTML
... 89 89. What is a Linear Feedback **Shift** Register? .... 90 90. What are **Shift** Register Cascades? ...
www.cs.rit.edu/~ats/inferno/web/labsfaq.pdf - Supplemental Result - Similar pages

[PDF] RSA Laboratories' Frequently Asked Questions About Today's ...
File Format: PDF/Adobe Acrobat - View as HTML
Page 1. Page 2. RSA Laboratories' Frequently Asked Questions About Today's

Cryptography, v4.0 2 Copyright © 1996, 1998 RSA Data Security, Inc. ...
www.directoryservice.com/WP/RSA/labsfaq4.pdf - Similar pages

[PDF] Capella University TS8999 ~ Special Topics in Technology ...
File Format: PDF/Adobe Acrobat - View as HTML
Page 1. Capella University TS8999 ~ Special Topics in Technology Guidelines for the Use Of Cryptography in the Enterprise Wolf M. Halton ...
www.networkdefense.biz/CryptoGuide.pdf - Similar pages

[DOC] CryptoGuide.Doc
File Format: Microsoft Word 2000 - View as HTML
... sent through the first rotor, which would **shift** the letter ... This principle of the **shifting** rotors allowed for 26X26X26 ... e, less than n and **relatively prime** to M ...
www.networkdefense.biz/CryptoGuide.doc - Similar pages

[PDF] Hardware implementation aspects of the Rijndael block cipher.
File Format: PDF/Adobe Acrobat - View as HTML
... Column symmetry in the row **shifting** operation is proven, closed ... 47 4.8 The Rijndael **Key Expansion**. ... of N b and N k . . . . . 41 4.2 **Shift** offsets for ...
rennes.ucc.ie/~cillian/files/ pubs/Rijndael-Implementation-Thesis.pdf - Supplemental Result - Similar pages

[PDF] RSA Laboratories FAQ (v3.0)
File Format: PDF/Adobe Acrobat - View as HTML
... 92 89. What is a Linear Feedback **Shift** Register? ... 93
90. What are **Shift** Register Cascades? ...
nicchia.ingce.unibo.it/nicchia97/ temi/sicurezza/labs_faq.pdf - Supplemental Result - Similar pages

[PDF] Εισαγωγή
File Format: PDF/Adobe Acrobat - View as HTML
... Choose a number, e, less than n and **relatively prime** to (p-1)(q-1), which means that ... There are three routines in RC5: **key expansion**, encryption, and decryption ...
www.conta.uom.gr/conta/ekpaideysh/metaptyxiaka/ technologies_diktywn/ergasies/Cryptography.pdf - Supplemental Result - Similar pages

Technique for reducing ...
... Figure 4 illustrates the process of **key expansion** in the rSA ... result is multiplied by 4 by **shifting** twice to ... a public key PK which is **relatively prime** to the ...
gauss.bacon.su.se/sql/view.php?p=EP202768 - 90k - Cached - Similar pages

[PS] Frames, Designs, and Spherical Codes in
File Format: Adobe PostScript - View as Text
... In the upper arm the beam acquires an l-dependent phase **shift** l` from the two Dove prisms, while a phase shifter imparts a fixed phase irrespective of mode ...
info.phys.unm.edu/~renes/publications/diss2side.ps.gz - Similar pages

[PS] Introduction to Modern Cryptography
File Format: Adobe PostScript - View as Text
... letting the first bit "fall off" (but remember it!) and **shifting** a zero ... **shift**-rows(s. 0. ... Figure 2.3: The AES128 **key-expansion** algorithm maps a 128-bit key K into ...
www.cs.ucdavis.edu/~rogaway/ classes/227/fall01/book/main.ps - Similar pages

In order to show you the most relevant results, we have omitted some entries very similar to the 26 already displayed.
If you like, you can repeat the search with the omitted results included.

relatively-prime shift OR shifting " Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Programs - Business Solutions - About Google

Published since January 1948 and Published before August 1999
Terms used **key expansion**

Found **4** of **96,589**

Sort results by: relevance
Display results: expanded form

Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 4 of 4

Relevance scale

1 Towards practical "proven secure" authenticated key distribution
Yvo Desmedt, Mike Burmester
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security**
Full text available: pdf(382.53 KB) Additional Information: full citation, abstract, references, citings, index terms

Secure key distribution is a critical component in secure communications. Finding 'proven secure' practical key distribution systems is one of the major goals in cryptography. The Diffie-Hellman variants, a family of key distribution systems, achieve some of the objectives of this goal. In particular, the 'non-paradoxical' system (by Matsumoto-Takashima-Imai and Yacobi) is claimed to be secure against a known-key attack. In this paper we show that the argument used to prove this is ...

2 A technique for integrated reports from a multi-run system
N. Budea, J. G. Kamena, R. M. Kamena
June 1965 **Communications of the ACM**, Volume 8 Issue 6
Full text available: pdf(401.56 KB) Additional Information: full citation, index terms

3 A proof of the security of quantum key distribution (extended abstract)
Eli Biham, Michel Boyer, P. Oscar Boykin, Tal Mor, Vwani Roychowdhury
May 1999 **Proceedings of the thirty-second annual ACM symposium on Theory of computing**
Full text available: pdf(968.70 KB) Additional Information: full citation, references, citings, index terms

4 Intelligent word-prediction to enhance text input rate (a syntactic analysis-based word-prediction aid for people with severe motor and speech disability)
Nestor Garay-Vitoria, Julio González-Abascal
January 1997 **Proceedings of the 2nd international conference on Intelligent user interfaces**
Full text available: pdf(423.65 KB) Additional Information: full citation, references, citings, index terms

Keywords: adaptation, chart technique, input speed enhancement, motor disabilities, syntax analysis, word-prediction

Results 1 - 4 of 4